UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

Joseph Van Loon; Tyler Almeida;
Alexander Fisher; Preston Van Loon;
Kevin Vitale; and Nate Welch,

Plaintiffs,

v.

Department of the Treasury;
Office of Foreign Assets Control;
Janet Yellen, in her official capacity
as Secretary of the Treasury; and
Andrea M. Gacki, in her official
capacity as Director of the Office
of Foreign Assets Control,

Defendants.

Civil Action No. 1:23-cv-00312-RP

BRIEF OF AMICUS CURIAE THE BANK POLICY INSTITUTE
IN SUPPORT OF DEFENDANTS' MOTION FOR SUMMARY JUDGMENT

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

STATEMENT OF INTEREST

The Bank Policy Institute (BPI) is a nonpartisan policy, research, and advocacy group that represents the nation's leading banks and their customers. BPI's member banks employ nearly two million Americans, make 68% of the nation's loans and nearly half of the nation's small business loans, and serve as an engine for financial innovation and economic growth.

BPI and its members are committed to a strong, inclusive, and resilient financial system that serves the national interest. That system, as it has developed over numerous years, includes strong protections for customer privacy that are enshrined in law. It also promotes ever-greater inclusion for the overwhelming majority of individuals, while denying services to select persons barred by applicable law, such as those who seek to engage in criminal activity, fund terrorism, launder money, or are the target of economic sanctions.

BPI has an interest in this case because it raises, including in briefs filed by *amici* supporting Plaintiffs, questions of how privacy and financial inclusion are protected and promoted in the regulated financial system as compared to other, newer systems that have developed for digital assets such as cryptocurrencies. BPI supports innovations in the financial sector but within the boundaries necessary to protect the rights, welfare, and safety of the Nation's citizenry. BPI has significant knowledge of, and experience with, the privacy and financial inclusion rules and practices applicable to the U.S. financial system, and can bring to the Court's attention context that may not otherwise be provided by the parties or the other *amici*.

INTRODUCTION AND SUMMARY OF ARGUMENT

The thrust of the argument made by Plaintiffs and their *amici* supporters is that we must be free to perform financial transactions in an unregulated environment because the regulated financial system does not provide sufficient privacy or inclusion. Both the premise and conclusion are wrong. As for the invalid premise, the regulated financial system does—and is legally required to—provide comprehensive privacy and ever-increasing inclusion for its current and prospective customers. As for the invalid conclusion, Congress has made the decision, which has been implemented by financial institutions and upheld by courts, *see Cal. Bankers Ass'n* v. *Shultz*, 416 U.S. 21 (1974), that our citizens' right to privacy is extensive but must be subject to the limited oversight necessary to protect them.

The regulated financial system in which BPI's members operate provides safe, efficient, and privacy-protected financial services to billions of customers around the world. In this system, financial institutions act as trusted service providers for their customers, and customers rely upon those institutions to keep their assets safe and personal information private. To ensure that financial institutions fulfill these responsibilities, they are subject to a comprehensive set of legislative and regulatory requirements, including extensive supervision. Regulated financial institutions around the world generally must comply with, among numerous other obligations, safety and soundness provisions, customer privacy requirements, "know your customer" and other anti-money laundering ("AML") rules, and applicable economic sanctions provisions. And in the United States, as in many jurisdictions, banks and other institutions are required to welcome customers regardless of their race, religion, or background and are prohibited from unlawfully discriminating against actual or prospective customers. *See, e.g.*, 42 U.S.C. § 3605(a) (Fair Housing Act); 15 U.S.C. § 1691(a) (Equal Credit Opportunity Act); N.Y. Banking Law § 9-F.

The regulated financial system is innovating at a record pace, introducing, among other enhancements, mobile payments and faster payment processing to enable customers to move money instantly. More and more individuals are joining the regulated banking system each year. According to the latest World Bank survey, 76% of the world's adults have a bank or mobile account, up from 51% in 2011. Asli Demirgüç-Kunt et al., *World Bank Group, The Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19*, at 2 (2022), https://www.worldbank.org/en/publication/globalfindex/Report. And in the United States, only 4.5% of households remain "unbanked," a record low. FDIC, *2021 FDIC National Survey of Unbanked and Underbanked Households* 12 (2021), http://www.fdic.gov/analysis/household-survey/2021execsum.pdf.

Ignoring all of these realities, Plaintiffs and their *amici* distort the legal framework and practices of regulated financial institutions in a bid to suggest that the only secure and accessible means to conduct financial activity are cryptocurrency transactions shielded by mixers like Tornado Cash. In particular, they suggest that regulated institutions (a) do not adequately protect customer privacy and (b) fail to practice financial inclusion. According to Plaintiffs' *amici*, financial institutions contribute to a "world of increasing threats to privacy" (ECF No. 59 Ex. A, Br. of Andreessen Horowitz as Amicus Curiae in Support of Pls's Mot. for Partial Summ. J., at 10 ("A16z Br.")), deprive customers of important financial freedom, and leave many without any services at all because they have been "historically discriminatory" (ECF No. 49, Br. of Blockchain Ass'n and DeFi Educ. Fund as Amici Curiae in Support of Pls's Mot. For Partial Summ. J. at 3 ("Blockchain/DeFi Br.")).

Plaintiffs and *amici* thereby provide the Court with a false and binary choice: between complete anonymity and unfettered access to financial services on the one hand and total public

disclosure and discriminatory barriers to entry—purportedly supplied by regulated financial institutions—on the other. Such descriptions of the regulated banking sector are flatly incorrect, and of course, the realities of financial inclusion and privacy are not a binary choice between two extremes.

Over the past fifty years, Congress and successive U.S. presidential administrations have built and enhanced a framework for the regulated financial system that carefully balances the inevitable tensions between privacy and public safety and security. Banks and other regulated institutions are required—on pain of civil and criminal penalties—to safeguard customer privacy, but also to monitor customer transactions for criminal activity, such as narcotics or human trafficking. Banks and other regulated institutions must also foster financial inclusivity by serving customers from all races, religions, and creeds, providing access to financial services that has helped lift countless individuals around the globe out of poverty. At the same time, they are legally required to exclude from the financial system certain actors, such as government-designated financiers of terrorist movements.

Plaintiffs and *amici* are obviously free to disagree as a policy matter with the approach set out by elected officials and regulators over decades, and to advocate for a new financial regime that places no limits on who may participate or the activities they may fund. That posture is decidedly not, however, the approach embodied in generations of U.S. laws and regulations and the judicial decisions that enforce and interpret those laws, nor does it comport with international standards, or the laws of any other democratic government worldwide of which we are aware.

Ultimately, BPI does not take a view in this brief as to how the designation authorities of the Treasury Department's Office of Foreign Assets Control apply to a mixer structured like Tornado Cash. But any insinuation that banks and other regulated institutions as an industry

engage in discrimination or otherwise ignore their legal obligations is untenable. Although, as in any human arena, there may be isolated legal violations, it is highly misleading to ignore the practices of the great majority of regulated financial institutions, which spend billions of dollars each year to protect customer privacy and promote financial inclusion, while instituting safeguards to protect their customers and the financial system as a whole from criminal activities.

ARGUMENT

I. FINANCIAL PRIVACY DOES NOT EQUATE TO ABSOLUTE ANONYMITY AND FINANCIAL INSTITUTIONS SAFEGUARD THEIR CUSTOMERS' PRIVACY IN ACCORDANCE WITH THEIR LEGAL OBLIGATIONS.

Plaintiffs and their *amici* repeatedly suggest that Tornado Cash and similar technologies are necessary to protect "financial privacy" but misconstrue what that term means and has always meant. In the context of financial transactions, privacy signifies the right of a person to have her account and transactional information protected against unauthorized disclosure to the public or to government authorities, absent a court-issued subpoena or other valid legal basis for such disclosure. In contrast, Plaintiffs and their *amici* utilize the term "financial privacy" as a euphemism for *anonymity*—a system in which a person can move hundreds of thousands of dollars across borders to anyone they wish, and the governments of jurisdiction would have no ability to determine the identity of the originator or beneficiary. Blockchain/DeFi Br. 3; A16z Br. 7; ECF No. 50 (Br. of Paradigm Operations LP as Amicus Curiae in Support of Pls's Mot. for Partial Summ. J) at 11. This novel use of the term "financial privacy" would be unrecognizable to governments, courts or international expert bodies the world over.

U.S. law and international financial standards set by the Financial Action Task Force (FATF)—a global body that issues recommendations concerning AML and countering the financing of terrorism, to which over 200 countries and jurisdictions worldwide have committed themselves—provide that banks must protect the financial privacy of their customers while also

complying with applicable laws that authorize disclosure to government officials with a subpoena. That legal landscape is aimed at, among other things, detecting and disrupting illicit activity and terrorist financing. There has never been a time when U.S. law recognized "financial privacy" as an absolute right to anonymity, even from government investigations. *See, e.g.*, *United States* v. *Miller*, 425 U.S. 435, 444 (1976) (issuance of a subpoena to a third party to obtain bank records does not violate depositor's Fourth Amendment rights). To do so would open the U.S. financial system to state and non-state actors who pose serious threats to our individual and national security.

A. Banks Are Subject to and Comply with Extensive Data Privacy Obligations.

Amici for Plaintiffs accuse "large financial institutions" of "sell[ing] Americans' financial and transaction data," as part of a "world of increasing threats to privacy." A16z Br. 10; *see also* Blockchain/DeFi Br. 5 (arguing that blockchain technology is necessary because "the need for privacy is heightened for certain, particularly sensitive transactions"). To the contrary, regulated financial institutions are required by a constellation of federal and state laws to provide financial privacy to their customers. *See, e.g.*, Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809 (generally prohibiting financial institutions from, *inter alia*, disclosing nonpublic personal information about a consumer to nonaffiliated third parties); Right to Financial Privacy Act, 12 U.S.C. § 3403(a) (providing that "no financial institution . . . may provide to any Government authority access to or copies of, or the information contained in, the financial records of any customer except in accordance with the provisions of this chapter"); 23 CRR-NY § 500.3(k) (firms operating pursuant to a New York Department of Financial Services license must implement and maintain policies and procedures that cover, among other things, customer data privacy); Tex. Fin. Code § 59.006 (providing the "exclusive method for compelled discovery" of the financial records of any customer).

The consumer financial privacy mandated by law is strictly enforced. For example, banks are routinely examined by supervisors to ensure they are safeguarding customer privacy appropriately. *See* FDIC, Consumer Compliance Examination Manual VIII (2021), https://www.fdic.gov/resources/supervision-and-examinations/consumer-compliance-examination-manual/documents/8/viii-1-1.pdf. Any institution that improperly discloses its customers' data may face steep fines, the loss of its banking license, and even criminal prosecution. *See* 12 U.S.C. § 1818(a)(2), (i)(2) (authorizing the termination of deposit insurance and civil money penalties with respect to banks that violate any law); Stipulated Order for Permanent Injunction and Monetary Judgment, *FTC* v. *Equifax, Inc.*, No. 1:19-cv-032 (N.D. Ga. July 23, 2019) (entering $579 million judgment against Equifax as part of settlement concerning data breach that resulted in the disclosure of customer information).

Financial institutions go to extraordinary lengths to protect consumer privacy. U.S. banks, including BPI's members, spend billions of dollars yearly on training, systems, and operational policies to protect their customers' data privacy as required by law. *See* Anupam Chander et al., *Achieving Privacy: Costs of Compliance and Enforcement of Data Protection Regulation* 24 (World Bank Group, Policy Research Working Paper No. 9594, 2021) (estimating that the financial industry spends $2-5 billion annually to comply with the Gramm-Leach-Bliley Act's privacy provisions alone). BPI and its members' commitment to consumer privacy, however, goes well beyond their legal obligations. BPI and its members have repeatedly championed consumer data privacy as a critical consideration whenever Congress considers updating the bank regulatory framework. *See Preserving the Right of Consumers to Access Personal Financial Data : Hearing Before the Task Force on Fin. Tech. of the H. Comm. on Fin. Servs.*, 117th Cong. 119 (2021)

(Written statement of the Bank Policy Institute) (arguing that "*informed consumer consent* should be a precondition to any sharing of consumer financial information").

Ultimately, financial institutions' privacy safeguards have proved effective. Consumers are well aware of this reality. According to a BPI survey conducted in 2019, 75% of U.S. voters were confident in the ability of their bank to securely collect and protect their personal data. BPI, Data Privacy Survey (2019), http://bpi.com/wp-content/uploads/2021/03/BPI-Banks-are-Trusted-with-Data-Privacy.pdf. Voters were three times more likely to trust banks and financial institutions to collect and protect their personal data than they were to trust technology companies. *Id.*

B. U.S. Law Requires Financial Institutions to Monitor for and Report Suspicious Activity While Protecting Consumer Information.

Even as financial institutions are required to protect and defend consumer privacy from public disclosure, they are also required under U.S. law to monitor customer transactions and to identify and report suspicious transactions. Congress has determined that transaction monitoring and reporting is "highly useful" for law enforcement and national security initiatives, including to prevent money laundering and terrorist financing. 31 U.S.C. § 5311(1). Money laundering is indisputably a serious problem, providing the "financial fuel that permits transnational criminal enterprises to conduct and expand their operations." 31 U.S.C. § 5311 note.

Beginning with the enactment of the Bank Secrecy Act of 1970 ("BSA"), Congress has required banks and other financial institutions to take action to combat the previous "heavy utilization of our domestic banking system by the minions of organized crime." *Shultz*, 416 U.S. at 30 (citing Pub. L. No. 91-508, 84 Stat. 1114). Today, financial institutions' obligations under the BSA and other AML laws and regulations are extensive. As part of implementing those programs, financial institutions must, among other things, file reports on transactions they identify as suspicious, 31 U.S.C. § 5318(g); 61 Fed. Reg. 4326 (Feb. 5, 1996); verify the identities of their

customers, 31 U.S.C. § 5318(l); and conduct due diligence on those customers to better understand the nature and purpose of customer relationships and transactions, *see, e.g.*, 31 C.F.R. § 1020.210(a)(2)(v). In addition, banks screen customer accounts and transactions in order to comply with U.S. economic sanctions, which bar entry to the U.S. financial system to numerous national security threats—including governments like the Democratic People's Republic of Korea, terrorist organizations like Al-Qaeda, and narcotics traffickers like the Sinaloa Cartel. *See generally* 31 C.F.R. ch. V; U.S. Dep't of Treasury, Office of Foreign Assets Control, *A Framework for OFAC Compliance Commitments* (May 2, 2019), https://ofac.treasury.gov/media/16331/download?inline.

The same basic regulatory structure exists across the world. For example, all 193 United Nations member states are obligated to pass laws mandating that their financial institutions deny services to certain sanctioned groups and persons, like Al-Qaeda, ISIS, and the Strategic Rocket Force of the Korean People's Army. *See* United Nations Security Council, *United Nations Security Council Consolidated List* (May 14, 2023), List of updates to the UNSC Consolidated List | United Nations Security Council; U.N. Charter art. 41, Ch. VII (explaining role and authority of the U.N. Security Counsel). To state the obvious, unless a financial institution can identify the true party to a transaction, it cannot comply with these global sanctions.

Although AML and sanctions programs are recognized by banks as essential, they require massive expenditures, which may explain why Plaintiffs' *amici* and others seek to avoid them. A BPI survey of 17 member institutions found that, as of 2017, they were collectively employing over 14,000 individuals and deploying up to 20 information technology systems to assist in BSA/AML compliance; 14 of these institutions together were investing approximately $2.4 billion on these efforts. BPI, *Getting to Effectiveness: Report on U.S. Financial Institution Resources*

Devoted to BSA/AML & Sanctions Compliance 2 (2018), https://bpi.com/wp-content/uploads/2018/10/BPI_AML_Sanctions_Study_vF.pdf.

In the briefs of Plaintiffs and their *amici*, they allude to general "privacy" interests afforded to users of Tornado Cash. In doing so, Plaintiffs and *amici* appear to adopt a new definition of financial privacy, one under which customers would enjoy absolute anonymity even from governments and courts and regardless of the types of activities in which those customers are engaged. *See, e.g.*, Blockchain/DeFi Br. 5 ("[D]igital asset users often prioritize anonymity when supporting politically charged causes, for fear of reprisal or government sanction."). As any informed discussion of the BSA/AML regulatory regime makes clear, however, privacy in financial activities is not synonymous with anonymity. To the contrary, anonymity is anathema to the global regulatory landscape under which institutions are required to track customer activity, flag potentially illicit action, and refuse to process transactions that violate sanctions and other laws. *Amici* are thus wrong to suggest that tools like Tornado Cash "allow users to reclaim privacy that would be available as a matter of course in other contexts." *Id.* at 4. There is no other context in which U.S. law extends complete anonymity to persons in the use of the financial system.[1]

There are obvious policy tensions here between individual privacy and national security. As with many public policy debates, the United States and other democratic governments have found their way to a middle course, neither permitting absolute anonymity nor resigning

[1] While some *amici* posit that cash transactions are anonymous, *see, e.g.*, A16z Br. 10, that is also incorrect. Financial institutions' suspicious activity reporting obligations also cover suspicious cash transactions, and even non-financial institutions must report cash transactions of over $10,000 in cash which must be recorded. *See* FFIEC Examination Manual, *Suspicious Activity Reporting* 66 (2015), https://bsaaml.ffiec.gov/docs/manual/06_AssessingComplianceWithBSARegulatoryRequirements/04.pdf; IRS, *Form 8300 and Reporting Cash Payments of Over $10,000* (Aug. 19, 2022), http://www.irs.gov/businesses/small-businesses-self-employed/form-8300-and-reporting-cash-payments-of-over-10000.

themselves to a world without privacy. The U.S. Congress and regulators have built and adjusted over time a sophisticated system that protects consumers, but gives government and financial institutions a tailored obligation to depart in a limited way from complete privacy protection in situations where Congress believes it fundamentally necessary. To the extent Tornado Cash aims to provide an absolutist financial system where all parties can transact without any rules, restrictions, or safeguards, and with no ability for the government to detect and prevent illicit activity, that is decidedly not the choice that the U.S. Congress, other governments, or international bodies have made.

II. BANKS SUPPORT FINANCIAL INCLUSION WHILE THWARTING ILLICIT ACCESS TO THE BANKING SYSTEM AS REQUIRED BY LAW.

Amici supporting Plaintiffs offer a similarly extreme re-interpretation of the concept of "financial inclusion" in a bid to explain the advantages of transactions outside the regulated financial system like those involving cryptocurrencies and mixers such as Tornado Cash. Cryptocurrencies and mixers, they assert, "provide safe, low-cost access for people of any race, nationality, or background to conduct transactions." A16z Br. 5. *Amici* suggest in contrast that banks and other regulated financial institutions do not support financial inclusion in the same way and have been "historically discriminatory." Blockchain/DeFi Br. 3.

Yet again *amici* offer a false choice, this time between a lawless system in which *any* actor can access the global financial system on the one hand and "discriminat[ion]" on the other. By contrast, the internationally accepted meaning of the term "financial inclusion" is the promotion of banking access for underbanked and unbanked persons around the world, *while abiding by* international and domestic laws like sanctions that exclude dangerous actors. *Amici*'s contorted use of "financial inclusion" is inconsistent with the accepted use of the term and clearly incompatible with U.S. law. Congress, regulators, and BPI's members have worked continuously

to expand financial inclusion, without compromising on the notion that selected threat actors should be denied access to the global financial system. We are aware of no argument, except possibly by *amici* here, that a denial of access to the financial system to criminals and terrorists effectuates "discrimination."

A. Regulated Financial Institutions Support and Are Critical to Efforts to Expand Financial Inclusion.

BPI and its members support without reservation efforts to increase financial inclusion. According to the Treasury Department, "[p]romoting financial inclusion and equity are key goals of U.S. economic policy." U.S. Dep't of Treasury, *The Future of Money and Payments 37* (2022), https://home.treasury.gov/system/files/136/Future-of-Money-and-Payments.pdf. "Access to safe, affordable, and sustainable insured transaction and savings accounts, along with quality financial education," the Federal Deposit Insurance Corporation has said, "improves consumers' ability to safely save, build assets, and create wealth." FDIC, *Economic Inclusion* (Apr. 27, 2023), https://www.fdic.gov/resources/consumers/economic-inclusion/index.html. The U.S. government and various international organizations of which the United States is a member have important initiatives underway to foster an inclusive financial system. *See, e.g.*, Press Release, U.S. Dep't of Treasury, U.S. Treasury Announces New Funding and Financial Services Headed to Underserved Communities (Feb. 28, 2023), https://home.treasury.gov/news/press-releases/jy1312; Global Partnership for Financial Inclusion, *G20 2020 Financial Inclusion Action Plan* (2020), https://www.gpfi.org/sites/gpfi/files/sites/default/files/G20%202020%20Financial%20Inclusion%20Action%20Plan.pdf. These governmental programs require partnership and concerted effort by the banking sector.

Banks must comply with numerous requirements designed to promote financial inclusion. The Community Reinvestment Act, for example, requires banks to "demonstrate that their deposit

facilities serve the convenience and needs" of their communities and to "help meet the credit needs" of those communities. 12 U.S.C. § 2901(a)(1), (3). Regulators examine banks to assess their "record of meeting the credit needs of [their] entire communit[ies]," publishing a detailed report of each bank's community reinvestment activities and assigning individual bank ratings. 12 U.S.C. § 2903.

The banking industry's activities in this area are notable and wide-ranging. For example, the banking industry in the United States has pursued collaboration with the Cities for Financial Empowerment Fund to support the "Bank On" initiative. As a result, over 200 banks now offer low-cost bank transaction accounts with features appropriate for individuals currently outside the mainstream financial system. *See* Paul Calem & Yasmeen Abdul-Razeq, BPI, *"Bank On" Transaction Accounts Helped Support Financial Inclusion During the Pandemic* (Sept. 22, 2022), https://bpi.com/wp-content/uploads/2022/09/Bank-On-Transaction-Accounts-Helped-Support-Financial-Inclusion-during-the-Pandemic.pdf. Individual banks also engage in various activities to support access, including in their products and philanthropic activities. *See*, *e.g.*, BPI, *The Time Is Now: 30 Best Bank Practices to Help Improve Outcomes in Black Communities* (2021), https://bpi.com/wp-content/uploads/2021/06/The-Time-is-Now-30-Best-Bank-Practices-to-Help-Improve-Outcomes-in-Black-Communities.pdf.

Further, notwithstanding one *amicus*'s accusation that regulated institutions have been "historically discriminatory" (Blockchain/DeFi Br. 3), banks do not, and legally may not, turn away customers based on race, religion or other protected characteristics. For example, banks may not discriminate based on protected characteristics in extending mortgages or other loans. *See, e.g.*, 42 U.S.C. § 3605(a) (Fair Housing Act); 15 U.S.C. § 1691(a) (Equal Credit Opportunity Act). They also are subject to various generally applicable federal and state antidiscrimination

requirements. *See, e.g.*, 42 U.S.C. § 1981; N.Y. Exec. Law § 296(2)(a) (New York State Human Rights Law); Cal. Civil Code § 52(a) (California Unruh Civil Rights Act).

Banks have comprehensive programs to comply with these requirements, which are subject to frequent regulatory examination. *See, e.g.*, CFPB, *Supervision and Examination Manual: Overview* 3–4 (2012), https://files.consumerfinance.gov/f/201210_cfpb_supervision-and-examination-manual-v2.pdf?source=post_page; Federal Reserve, *Consumer Compliance Handbook* iii (2013), https://www.federalreserve.gov/boarddocs/supmanual/cch/cch.pdf (describing CFPB and Federal Reserve consumer compliance oversight and examinations); OCC, *Fair Lending: Revised Comptroller's Handbook Booklet and Rescissions* (Jan. 12, 2023), https://www.occ.treas.gov/news-issuances/bulletins/2023/bulletin-2023-2.html. A violation of antidiscrimination requirements may lead a bank to face substantial liability, including fines. *See, e.g.*, Consent Order, *United States* v. *City Nat'l Bank*, No. 2:23-cv-00204 (C.D. Cal. Jan. 30, 2023) at Dkt. 20 (settlement with the Justice Department relating to alleged lending discrimination requiring a bank to pay $31 million in relief); Consent Order, *United States and CFPB* v. *Trustmark National Bank*, No. 2:21-cv-2664 (W.D. Tenn. Oct. 27, 2021) at Dkt. 26 (settlements with the Justice Department, CFPB and OCC providing for a $5 million aggregate penalty and a $3.85 million loan subsidy program); Consent Order, *United States* v. *Cadence Bank, N.A.*, No. 1:21-cv-03586 (N.D. Ga. Aug. 31, 2021) at Dkt. 4 (settlements with Justice Department and OCC providing for among other things, $3 million penalty and over $5.5 million in loan subsidies and other initiatives).

The partnership between the government and banks in the United States to advance financial inclusion has made notable progress, as described above. The percentage of U.S. households that remain "unbanked" is at a historic low of 4.5%, FDIC, *2021 FDIC National*

Survey of Unbanked and Underbanked Households 12, *supra*, and the number of adults globally without a bank or similar account declined by over a billion between 2011 and 2021. World Bank, *Financial Inclusion Overview* (Mar. 29, 2022), https://www.worldbank.org/en/topic/financialinclusion/overview. BPI and its members see this progress as notable but unfinished and are committed to extending financial inclusion further in the years to come.

B. Promoting Financial Inclusion Does Not Mean Allowing Criminal and Sanctioned Actors to Have Indiscriminate Financial Access.

The promotion of financial inclusion, however, does not mean that anyone is entitled to obtain a financial account and move funds across borders for any reason. As with financial privacy, elected lawmakers have established a balance between important but competing policy interests. Indeed, Congress has imposed numerous requirements to ensure that banks and other regulated financial institutions do *not* do business with those whom the government has identified as serious threats to the United States and its citizens. U.S. law requires that all companies and persons—including financial institutions—deny access, goods, and services to sanctioned parties, outside of certain carefully delimited categories or individual transactions determined by the U.S. government to be consistent with current U.S. policy.

A vital aspect of these efforts is the obligation of financial institutions to understand who their customers are—obligations generally referred to as "know-your-customer" or "KYC." KYC obligations for banks were imposed in the United States when the BSA was first introduced and have expanded since. In addition to banks, financial institutions required to perform KYC now include, among others, securities broker-dealers, money transmitters, and casinos. 31 U.S.C. § 5312(a)(2). In 2001, Congress amended the BSA to require that certain financial institutions, including banks, "verify[] the identify of any person seeking to open an account to the extent reasonable and practicable" and "consult[] lists of known or suspected terrorists or terrorist

organizations" to determine if the person appears on such a list. USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 326, 115 Stat. 272, 317 (codified at 31 U.S.C. § 5318(*l*)). The Financial Crimes Enforcement Network ("FinCEN"), a Treasury bureau focused on combating money laundering, has historically recognized that KYC activities of financial institutions require them to conduct comprehensive due diligence on their customers, 77 Fed. Reg. 13,046 (Mar. 5, 2012), and those expectations were clarified and codified in a formal customer due diligence rule that became effective in 2018. 81 Fed. Reg. 29,398 (May 11, 2016); 31 C.F.R. §§ 1010, 1020, 1023, 1024, 1026.

KYC has become a bedrock underpinning of a safe financial system not just in the United States, but globally. FATF, for example, describes KYC as a fundamental building block to effectively combat money laundering and terrorist financing. FATF, *The FATF Recommendations* 13-14 (2023), https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf. The need for KYC is foundational to a host of other measures that financial institutions are required to implement. If a financial institution does not know who its customers are, it will be unable to identify whether any of those customers are, for example, sanctioned leaders of North Korea's Office 39[2] or of a murderous terrorist group. While sanctioned persons and other bad actors might welcome this type of system, democratic societies decidedly do not. Similar to checking passports at a border, if gatekeepers cannot identify the true identity of a person seeking to enter a country, they have no

[2] Office 39 is "a secretive branch of the government of North Korea that engages in illicit economic activities and generates revenues for North Korean leadership." Press Release, U.S. Dept' of Treasury, Treasury Sanctions Individuals and Entities Supporting the North Korean Government and its Nuclear and Weapons Proliferation Efforts (Dec. 2, 2016), http://home.treasury.gov/news/press-releases/jl0677.

hope of denying access to persons banned from travel, as is required under U.N. Security Council sanctions or U.S. travel bans.[3]

Accordingly, financial inclusion—like financial privacy—has never been recognized as an absolute right that supersedes the safety of the citizenry, but rather a vital interest that requires certain limited impingement by other vital interests. As FATF describes it, financial systems must "respond[] to the need to bring the financially excluded into the regulated financial sector," but must also "maintain[] effective safeguards and controls against [money laundering and terrorist financing] risks." *See* FATF, *Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion* 4 (2017). This is the system that Congress, regulators, and other international jurisdictions have endorsed: a system where all persons that desire a bank account can get one with very narrow exceptions for superseding interests. *See* World Bank, *Financial Inclusion Overview*, *supra* ("Financial inclusion means that individuals and businesses have access to useful and affordable financial products and services . . . delivered in a responsible and sustainable way."). Any conception of financial inclusion that would involve, as Plaintiffs' *amici* suggest, making financial services available irrespective of criminal or terrorist affiliation is radical and unsupported by law. The U.S. financial system does not work that way, and one that did would not be "inclusive." It would be, in the view of most regulators worldwide, highly dangerous.

[3] We would note that the need for such safeguards would seem particularly urgent in the unregulated cryptocurrency arena addressed by *amici*, given the substantial participation of sanctioned parties and illicit actors. *See, e.g.*, FinCEN Consent Order, Number 2022-03, (Oct. 10, 2022), https://www.fincen.gov/sites/default/files/enforcement_action/2023-04-04/Bittrex_Consent_Order_10.11.2022.pdf (imposition of over $29 million penalty against crypto asset trading platform, Bittrex, Inc., in connection with 116,000 transactions, valued at over $260 million with entities and individuals operating from OFAC-sanctioned jurisdictions).

CONCLUSION

For these reasons, BPI urges the Court to disregard arguments by Plaintiffs and their *amici* supporters that purport to defend Tornado Cash and other mixers as necessary tools to safeguard financial privacy and inclusion.

Dated: May 17, 2023.

Respectfully submitted,

/s/ *John Kinchen*

John Kinchen
Federal ID No. 235595
Texas Bar No. 00791027
S.D. ID No. 18184
Smyser Kaplan & Veselka, L.L.P.
717 Texas Avenue, Suite 2800
Houston, Texas 77002
(713) 221-2345
jkinchen@skv.com

Counsel for Amicus Curiae

CERTIFICATE OF SERVICE

I hereby certify that on May 17, 2023, I caused the foregoing to be filed with the Clerk of Court upon all counsel of record via the CM/ECF system.

/s/ *John Kinchen*
John Kinchen